(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75761 A1

(51) International Patent Classification[7]: G06F 1/02, G06J 1/00

(21) International Application Number: PCT/US00/15932

(22) International Filing Date: 8 June 2000 (08.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/138,182 8 June 1999 (08.06.1999) US
09/455,951 7 December 1999 (07.12.1999) US

(71) Applicant *(for all designated States except US)*: GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tournament Drive, Horsham, Philadelphia, PA 19044 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: SPRUNK, Eric, J. [US/US]; 6421 Cayenne Lane, Carlsbad, CA 92009 (US).

(74) Agents: KULAS, Charles, J. et al.; Townsend and Townsend and Crew LLP, 8th floor, Two Embarcadero Center, San Francisco, CA 94111 (US).

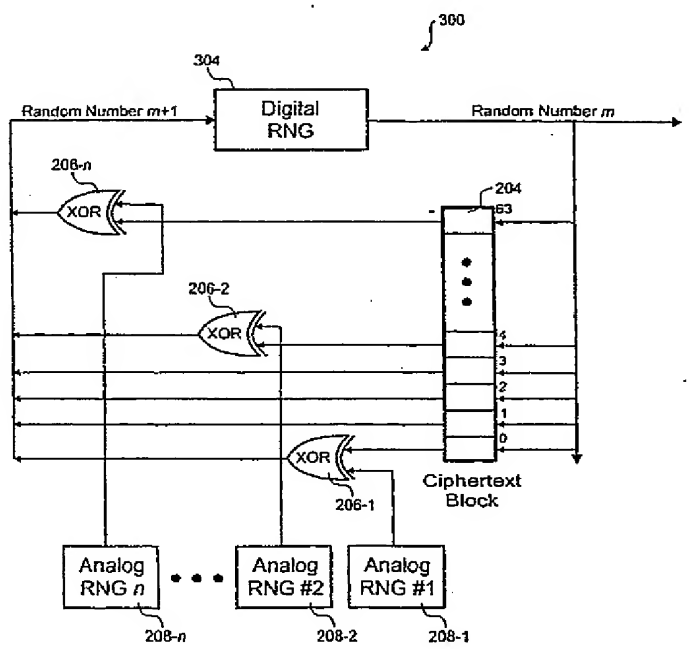
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: ROBUST RANDOM NUMBER GENERATOR



(57) Abstract: Methods and an apparatus (300) for generating random numbers are disclosed. In a first embodiment, a method for generating random numbers involves producing a second random number. A pseudorandom number is produced from a digital random number generator (304) and a first random number is produced from an anolog random number generator (208-1). The first random number is combined with the pseudorandom number to produce a second random number that is a result of both generators' outputs.

WO 00/75761 A1

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

ROBUST RANDOM NUMBER GENERATOR

This application claims the benefit of U.S. Provisional Application No. 60/138,182 filed on June 8, 1999.

BACKGROUND OF THE INVENTION

This invention relates in general to random number generators and more specifically to random number generators which use both digital and analog random number sources.

Random number generators are used for a variety of purposes such as cryptography. Correct use of cryptography depends on a statistically high quality source of random numbers. Unfortunately, conventional random number generators ("RNG") have disadvantages.

Simple random number generators use digital techniques to produce pseudorandom numbers. Pseudorandom numbers are substantially or highly random numbers which are produced by a digital process. Digital techniques can produce pseudorandom numbers which are deterministic because of their digital nature. In other words, two identical digital random number generators produce the same pseudorandom number when the digital input values are the same. Accordingly, digital techniques produce less than ideal results because the pseudorandom numbers are predictable.

A common digital technique for generating a random number is a linear congruential generator algorithm. This algorithm iterates to produce an output which is used as the seed for the next output. However, the sequence of random numbers produced by this technique is small and repeats after a relatively small number of distinct outputs. An orbit is defined herein as the number of outputs the digital random number generator produces until one output is the same as a previous output. As can be appreciated, a recursive algorithm will produce unique outputs in the orbit until an output is repeated. Once the first value repeats, the subsequent values will also be repeats. A

repeating pattern is undesirable since it is predictable. This algorithm is found in most C programming language libraries.

To provide robust random numbers, conventional systems rely upon analog random number generators. Analog random number generators produce a stream of random numbers which do not have a periodic orbit like the digital random number generators. These analog random number generators typically convert a random analog voltage, such as noise, into a digital stream of random data. These circuits are typically separate integrated circuits which generate a stream of random numbers at a rate of 100 Kbits or less. However, these random number generation rates are inadequate for very high performance cryptography, where a large number of random bits is needed in a short period of time.

Analog random number generators are prone to failure. The lifetimes of analog random number generators are considerably less than the digital circuits which use the random numbers. As can be appreciated by those skilled in the art, failure of the analog random number generator can defeat effective cryptology. Additionally, the source of the analog voltage used to generate the random number is vulnerable to control by an attacker. Accordingly, there is a need for more reliable analog random number generators which are less vulnerable to attack.

Analog random number generators are typically located on a separate integrated circuit from the digital circuits which use the random numbers because digital semiconductor processes are generally incompatible with analog semiconductor processes. Digital integrated circuits typically have high gain and are optimized for fast CMOS switching. However, analog random number generators require linear analog characteristics to effectively amplify the source of the random voltage in order to randomly produce a digital data stream. Modifying the digital semiconductor process to create better analog characteristics is possible, but the digital circuit performance would be adversely affected. Accordingly, integrating an analog random number generator on the same integrated circuit is very difficult with conventional techniques.

Additionally, an analog random number generator located on an integrated circuit separate from the integrated circuit containing the digital cryptographic function is prone to attack. More specifically, the trace on the circuit board which carries the random

number to the cryptographic function is vulnerable. For example, an attacker can manipulate or replace the signal from the analog random number generator. As those skilled in the art can appreciate, this attack would render the cryptographic algorithm and keys more easily determinable.

In summary, it is desirable to develop a random number generator which reliably produces random numbers at a high data rate. Additionally, the random number generator should accommodate integration with digital circuits on the same integrated circuit.

SUMMARY OF THE INVENTION

According to the invention, methods and an apparatus for generating random numbers are disclosed. In a first embodiment, a method for generating random numbers involves producing a second random number. A pseudorandom number is produced from a digital random number generator and a first random number is produced from an analog random number generator. The first random number is combined with the pseudorandom number to produce a second random number that is a result of both generators' outputs.

In another embodiment, a method generates a random number using a cryptographic function. A pseudorandom number is generated from an output of the cryptographic function and a first random number is generated from an analog random number generator. The pseudorandom number and the first random number are coupled to an input of the cryptographic function in order to generate a second random number from the output of the cryptographic function where the second random number is related to the pseudorandom number and first random number.

In yet another embodiment, a random number generator apparatus having an output, a digital random number generator and an analog random number generator. The digital random number generator produces a pseudorandom number. The analog random number generator generates a random number. The random number generator's output is coupled to both the digital and analog random number generators.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram representation of an embodiment of a random number generator which uses a cryptographic function;

Fig. 2 is a block diagram illustrating an embodiment of a random number generator which uses both analog random number generators and a cryptofunction to produce random numbers;

Fig. 3 is a block diagram representation of another embodiment of a random number generator which uses both analog and digital random number generation techniques;

Fig. 4 is a block diagram illustrating an embodiment of a random number generator which uses analog random number generation techniques to additionally randomize the key;

Fig. 5 is a block diagram illustrating an embodiment of a random number generator which uses analog random number generation techniques to randomize the key;

Fig. 6 is a block diagram representation of an embodiment of a random number generator which utilizes a hash function and a nonvolatile register; and

Fig. 7 is a flow diagram illustrating a method for generating a random number.

DESCRIPTION OF THE SPECIFIC EMBODIMENTS

While this invention is susceptible of embodiments in many different forms, there is shown in the drawings and will herein be described in detail, a number of embodiments of the invention with the understanding that the present disclosure is to be considered as an exemplification of the principles of the invention and is not intended to limit the broad aspects of the invention to the embodiment illustrated.

In the Figures, similar components and/or features have the same reference label. Various components of the same type are distinguished by following the reference label by a dash and a second label that distinguishes among the similar components in the same figure. If only the first reference label is used in the following disclosure, the description is applicable to any one of the several similar components.

One embodiment is illustrated in Fig. 1. This embodiment 100 produces blocks of pseudorandom numbers using a cryptographic function 104 or cryptofunction to encrypt in a loop. Included in the cryptofunction 104 is a plaintext input, a key input and a ciphertext output. The ciphertext output is used as the pseudorandom number.

The key input receives a key which is used by the cryptofunction 104 to produce the ciphertext output. The key is initialized into the device once, and need not change during the lifetime of the random number generator 100.

The ciphertext output produces blocks of pseudorandom numbers one after another. Each block is fed back into the input of the cryptofunction 104 as the seed for the next encryption. The cryptofunction 104 can be any symmetric or asymmetric crypto algorithm. For example, the asymmetric crypto algorithm could be an asymmetric public key cipher. Additionally, the cryptofunction 104 could either encrypt or decrypt to produce the pseudo random numbers. Preferably, the crypto algorithm is a symmetric block cipher function which encrypts to produce the random numbers. An example of the symmetric block cipher function is the Data Encryption Standard (DES).

To increase the random state of the cryptofunction 104, a random number seed is used. The seed is preferably produced with a high grade analog random number generator. Having a random seed makes the values in the output orbit unpredictable. However, this embodiment will repeat the same distinct set of values in the orbit until the key is changed. The output appears random because for strong cryptofunctions 104 the orbit is very large.

To further increase the quality of the pseudorandom output, the speed of the cryptofunction 104 is accelerated beyond the speed at which the output is read. By running the cryptofunction 104 fast, two successive pseudorandom numbers read would be separated by pseudorandom numbers which could not be read. Hence, the output is decorrelated from the cryptofunction 104. As those skilled in the art can appreciate, this feature makes it more difficult for an attacker to determine the key or cryptographic algorithm by analyzing the output.

With reference to Fig. 2, another embodiment of a random number generator 200 is shown in block diagram form. Included in the random number generator 200 is a cryptofunction 104, a ciphertext block register 204, a number of analog random

number generators ("RNG") 208, and a number of exclusive OR (XOR) gates 206. This embodiment uses both a cryptofunction 104 and analog random number generators 208 to produce truly random numbers. Additionally, this embodiment is robust because failure of all the analog random number generators 208 will not ruin the random number generator 200. Failure of all analog random number generators would reduce the circuits effectiveness to that of the embodiment in Fig. 1.

The cryptofunction 104 produces a first random number (m) which is coupled to a ciphertext block register 204. The ciphertext register 204 can be a serial or parallel configured memory register which stores one sixty-four bit block of ciphertext from the cryptofunction 104. A delay of one random number generation time cycle is introduced by the ciphertext register 204.

When the random number (m) is leaves the register 204, preferably at least one bit is acted upon by the analog random number generator 208. As can be appreciated by those skilled in the art, modification of one bit will change the orbit of the cryptofunction 104. Accordingly, if one bit is changed by an analog random number generator per orbit, a repeating orbit will never occur. Preferably, some bits leaving the ciphertext register 204 are XORed with the output from the analog number generators 208. However, other embodiments could combine the output from the register 204 and the analog random number generator 208 in any number of ways.

The analog random number generators 208 are preferably on the same integrated circuit as the cryptofunction 104. However, they could equally be on another integrated circuit. The analog random number generators 208 variously convert heat, electrical noise, diode electron junction noise, phase noise from a phase locked loop, and/or metastable timing boundaries into a random binary data stream. If these generators 208 are produced on chip (i.e., on the same integrated circuit), they may be unreliable for the reasons explained above in the background section. If all of the generators 208 fail, the cryptofunction will use the last random number as a seed to pseudorandomly generate pseudorandom numbers with the cryptofunction 104 alone.

Each analog random number generator 208 produces an output which may modify a bit output from the ciphertext register 204. The output from the random number generator could be XORed with a bit of the register 204 or simply replace that bit. If the

analog random number generator 208 has stopped producing a random output, the effect of the generator 208 upon the register 204 is logically disabled to prevent reductions in randomness. One way to test the effectiveness of a generator 208 is to check for an even distribution of zeros and ones over time. Other techniques for testing the effectiveness of a generator 208 are also known. In other embodiments, the generator 208 could produce a number of bits for each ciphertext block and modify the same number of bits output from the register 204.

After the analog generators 208 introduce entropy into the random number (m), the result is a second random number (m+1). The second random number is coupled to the plaintext input of the cryptofunction 104 as a seed to produce a third random number (m+2). This cycle repeats to produce random number blocks in a cyclical fashion.

Referring next to Fig. 3, another embodiment of a random number generator 300 is illustrated in block diagram form. This embodiment is similar to the embodiment of Fig. 2, except the cryptofunction 104 is replaced with a digital random number generator 304. Preferably, a software algorithm serves as the digital random number generator 304, but other embodiments could use a hardware circuit. The resulting pseudorandom number from the generator 304 is deterministic. As discussed in the background section, software random number generators have short orbits. However, since analog randomness is introduced by the analog random number generators 208, this embodiment produces robust random numbers without a repeating orbit.

The digital random number generator 304 could be implemented in any number of ways. Preferably, a linear congruential algorithm is encoded in software and executed on a general purpose processor. However, this invention can increase the robustness of any digital random number generating technique.

With reference to Fig. 4, an embodiment of a random number generator 400 is shown in block diagram form. This generator 400 improves randomness by changing the key used in the cryptofunction 104 in addition to changing the bits output from the ciphertext block register 204. A digital random number generator which used a cryptofunction (for example, see Fig. 1) repeats an orbit so long as the key remains

unchanged. However, changing the key will change the relationship between the plaintext and ciphertext which also changes the orbit.

The key is stored in a key register 404 before loading into the cryptofunction 104. The analog random number generators 208 randomize bits input into the key register 404 by XORing 408 those bits with respective analog random number generators 208. Periodically, the randomized key is loaded into the cryptofunction 104. As can be appreciated, the actual value of the key is typically not important for the purposes of generating random numbers.

Referring next to Fig. 5, an embodiment of a random number generator 500 is shown which randomizes a key input into the cryptofunction 104. This embodiment is similar to the embodiment of Fig. 4 except analog random number generators 208 are not coupled to the encryption loop. The key input is randomized by coupling a number of analog random number generators to bits of the key through XOR gates. Periodically, the newly randomized key in the key register 404 is loaded into the cryptofunction 104. As can be appreciated by those skilled in the art, changing the key alters the repeating pattern of random numbers in the orbit produced by the cryptofunction 104.

With reference to Fig. 6, another embodiment of a random number generator 600 is illustrated as a block diagram. This generator 600 adds a non-volatile register 604 and a hash function 608 to further improve the random number quality.

The hash function 608 takes the output from the cryptofunction 104 and further scrambles the output. Preferably, a secure hash algorithm, such as SHA-1, is used. Those skilled in the art can appreciate that adding the hash function increases the security of the cryptographic algorithm and key from attackers by introducing a barrier to analysis in the form of the hash function's inherent one-way function.

To preserve the randomness in the orbit, a nonvolatile register 604 is used to periodically store a cipher text block. Preferably, the register 604 is battery backed random access memory (RAM), but could also be flash memory, magnetic core memory, electrically erasable read only memory, or other nonvolatile memory. Periodically, a processor (not shown) reads the cipher text block register 204 and stores that value in the nonvolatile register 604. When power is removed from the circuit, the nonvolatile

register 604 retains the last stored random number. Upon application of power, the processor reads the nonvolatile register 604 and loads that value into the ciphertext register 204. The recovered value is used as a seed for subsequent random number generation. Accordingly, any accumulation of randomness over time is substantially retained.

With reference to Fig. 7, a flow diagram is shown which depicts one method for producing a random number. In step 700, a determination is made whether this is the first power up of the random number generator. This could be determined by checking for a previously stored software variable or checking for a value in the nonvolatile register 604. If it is determined this is the first power up, a random number seed is loaded in step 704. Preferably, the seed number is generated external to the integrated circuit by a high quality analog random number generator. In the case where the random number was previously stored because this is not the first application of power, the nonvolatile register 604 is loaded in step 708.

Once the random number generator is initialized with a random seed, the generation of additional random numbers can proceed. In step 712, a random number is generated from the random seed. In step 728, a hash function is performed upon the random number. If any circuit or cryptographic operation requires a random number, it is used in step 732.

After a random number is generated in step 712, the next random number in the orbit is prepared. In step 716, the analog random number generators 208 mixes additional randomness into the random number. In step 720, the output is coupled to the plaintext input of the cryptofunction 104. Periodically, step 724 stores the present random number in nonvolatile register 604. A processor stores the present random number at infrequent intervals, such as once per second. In this way, the generator produces random numbers in a robust manner.

In light of the above description, a number of advantages of the present invention are readily apparent. The random number generator can produce pseudorandom numbers even if all analog random number generators fail. By not relying solely upon analog random number generation, integration of analog random number generators is practical in a digital semiconductor process even though the analog

generators may have poor initial characteristics and eventually fail. Additionally, high random number data rates are possible since the random number generator utilizes digital techniques.

A number of variations and modifications of the invention can also be used. In different embodiments, the random number generator can be modified in any one or more of the following ways. The cryptofunction could serve a dual role in providing both random numbers and encryption/decryption. Accordingly, the circuit which already has a cryptofunction would require little additional circuitry to also provide random number generation. Although the above embodiment discussed in relation to Fig. 6 periodically stores the random number for later use as a seed, other embodiments could store the random number after power is removed if adequate operating power is supplied internally by capacitors or a battery.

The foregoing description of the invention has been presented for the purposes of illustration and description and is not intended to limit the invention. Variations and modifications commensurate with the above description, together with the skill or knowledge of the relevant art, are within the scope of the present invention. The embodiments described herein are further intended to explain the best mode known for practicing the invention and to enable those skilled in the art to utilize the invention in such best mode or other embodiments, with the various modifications that may be required by the particular application or use of the invention. It is intended that the appended claims be construed to include alternative embodiments to the extent permitted by the prior art.

WHAT IS CLAIMED IS:

1. A method for generating random numbers, the method comprising steps of:

producing a pseudorandom number from a digital random number generator;

producing a first random number from an analog random number generator; and

combining the first random number with the pseudorandom number to produce a second random number that is a result of both generators' outputs.

2. The method according to claim 1, wherein the step of producing a pseudorandom number comprises a step of producing a pseudorandom number from a cryptographic function.

3. The method according to claim 1, further comprising a steps of:

periodically storing the second random number in a non-volatile memory location;

powering up the digital random number generator; and

loading the previously stored second random number into the digital random number generator.

4. The method according to claim 1, wherein the step of producing a pseudorandom number comprises executing a software algorithm on a processor.

5. The method according to claim 1, wherein the step of producing a pseudorandom number comprises producing a pseudorandom number block from a symmetric block cipher function.

6. The method according to claim 1, wherein the step of producing a pseudorandom number comprises producing a pseudorandom number from an asymmetric public key cipher function.

7. A method for generating a random number with a cryptographic function, the method comprising the steps of:

generating a pseudorandom number from an output of the cryptographic function;

generating a first random number from an analog random number generator;

coupling the pseudorandom number and the first random number to an input of the cryptographic function; and

generating a second random number from the output of the cryptographic function which is related to the pseudorandom number and first random number.

8. The method according to claim 7, wherein the cryptographic function and the analog random number generator are located in a same package.

9. The method according to claim 8, further comprising a step of storing the second random number in a non-volatile memory location.

10. The method according to claim 7, wherein the step of generating a pseudorandom number comprises a step of initializing the cryptographic function with a random number source.

11. The method according to claim 10, wherein the random number source is external to a package which comprises the cryptographic function and the analog random number generator.

12. The method according to claim 7, further comprising a step of loading a key into the cryptographic function.

13. The method according to claim 12, further comprising a step of coupling the analog random number generator to a bit of the key before the step of loading a key.

14. The method according to claim 7, wherein the step of generating a pseudorandom number comprises generating a pseudorandom number block from a symmetric block cipher function.

15. The method according to claim 7, wherein the step of generating a pseudorandom number comprises generating a pseudorandom number from an asymmetric public key cipher function.

16. A random number generator apparatus, comprising:

an output;

a digital random number generator which generates a pseudorandom number; and

an analog random number generator which generates a random number, wherein the output is coupled to the digital and analog random number generators.

17. The random number generator apparatus of claim 16, wherein the digital random number generator comprises a cryptographic function.

18. The random number generator apparatus of claim 17, wherein the cryptographic function produces pseudorandom numbers faster than the output is read.

19. The random number generator apparatus of claim 16, wherein the pseudorandom number is coupled to an input of the digital random number generator.

20. The random number generator apparatus of claim 16, further comprising a register having a plurality of bits which contains the pseudorandom number, wherein the analog random number generator is coupled to at least one of the bits.

21. The random number generator apparatus of claim 16, further comprising a plurality of analog random number generators.

22. The random number generator apparatus of claim 16, further comprising a hash function coupled to the output.

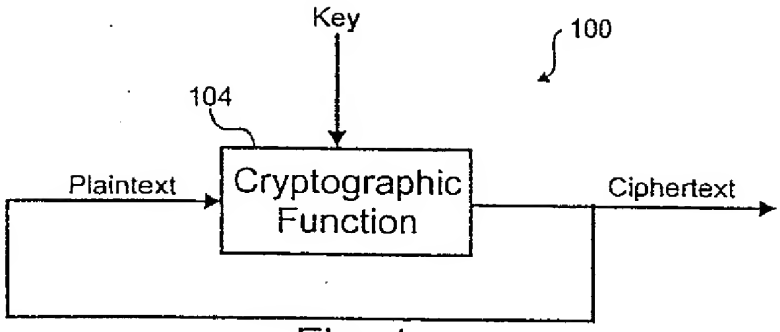


Fig. 1

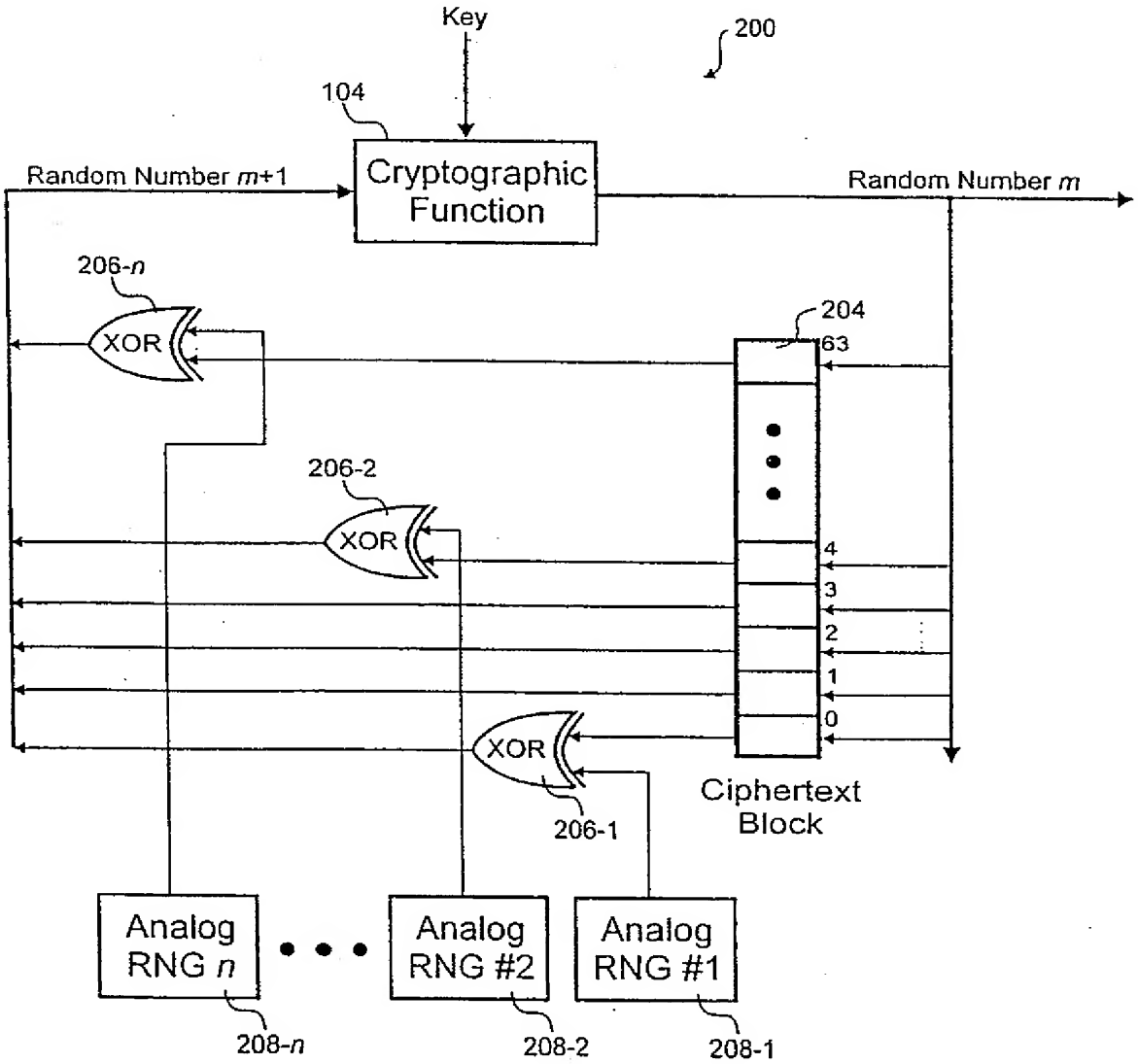


Fig. 2

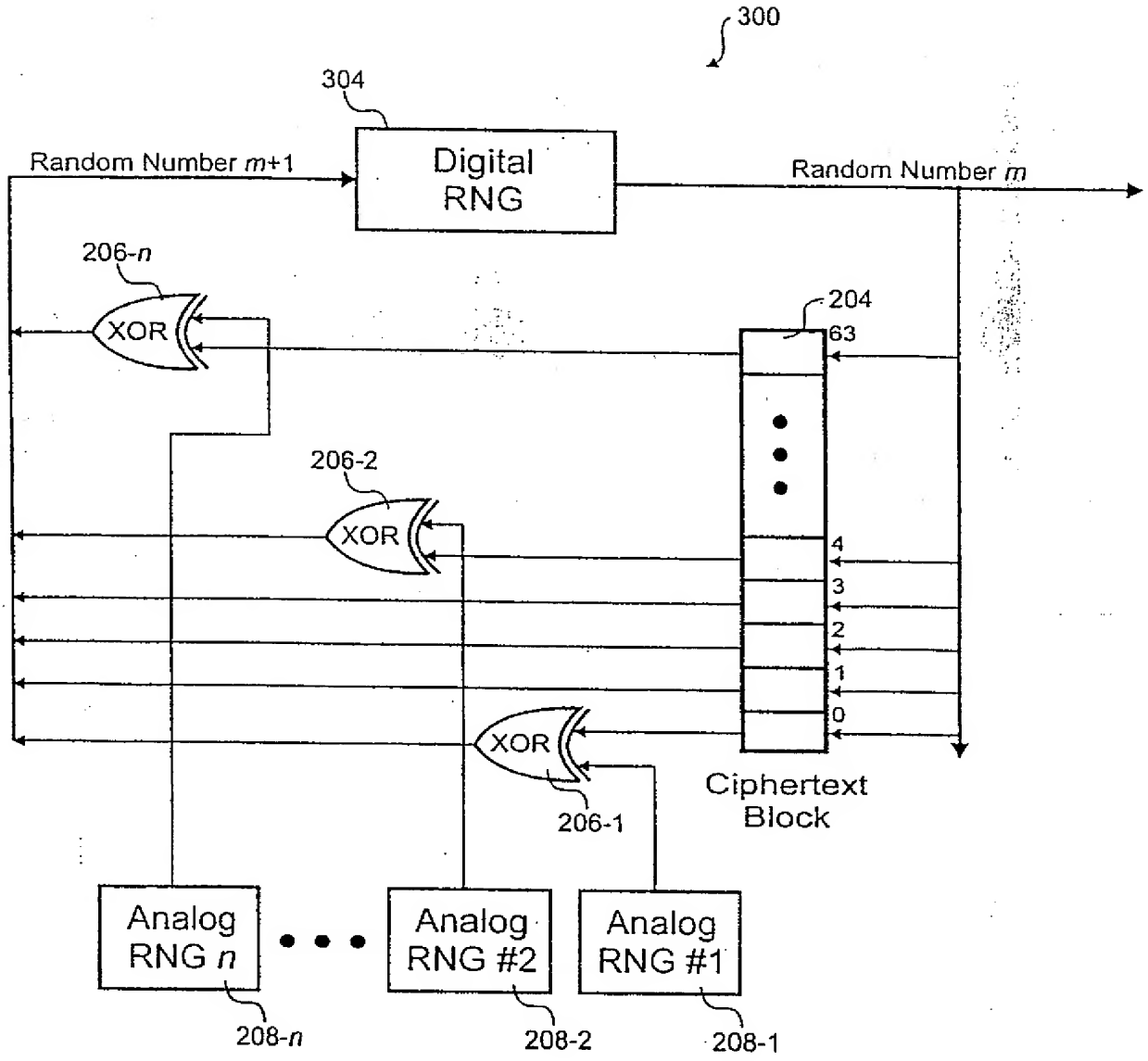


Fig. 3

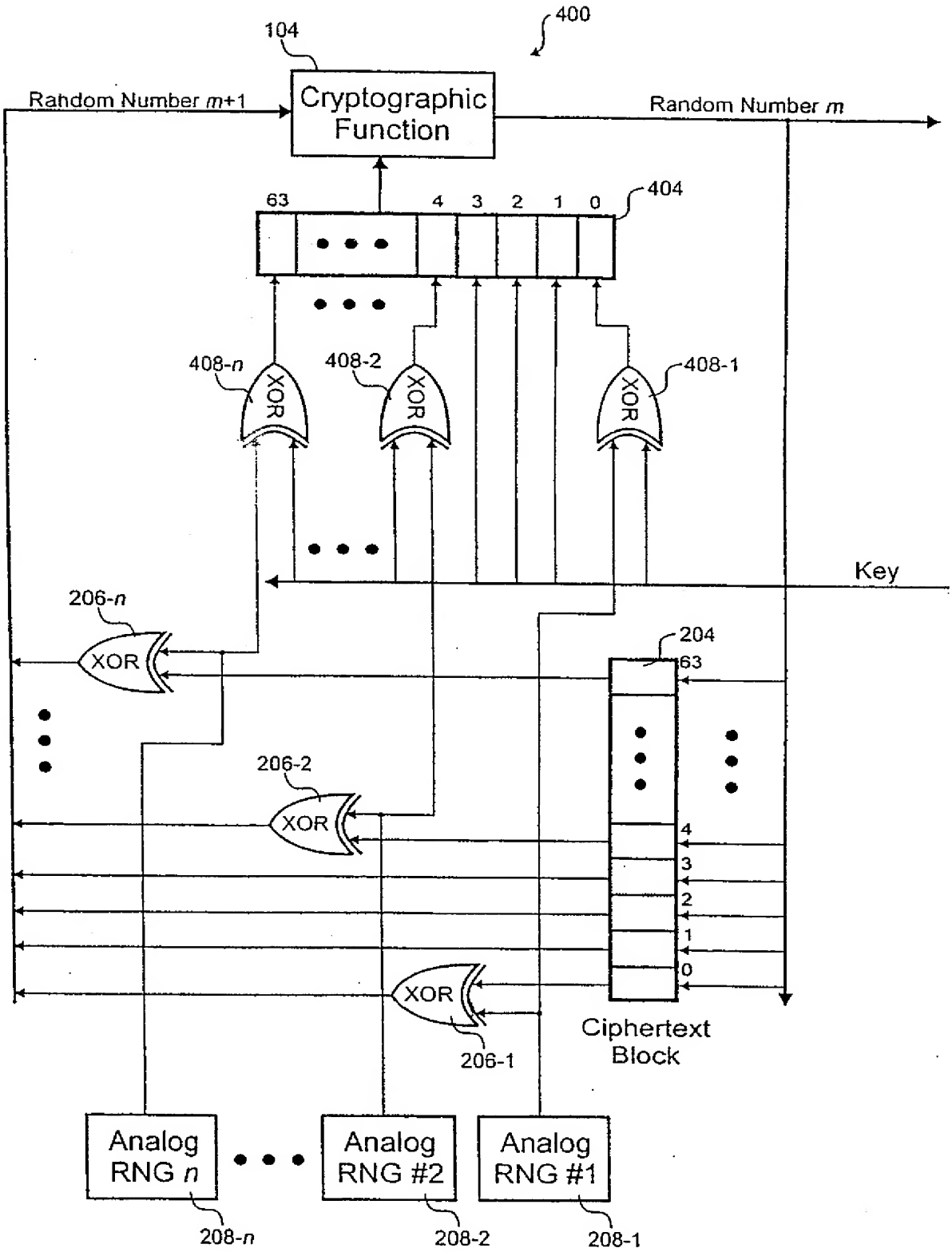


Fig. 4

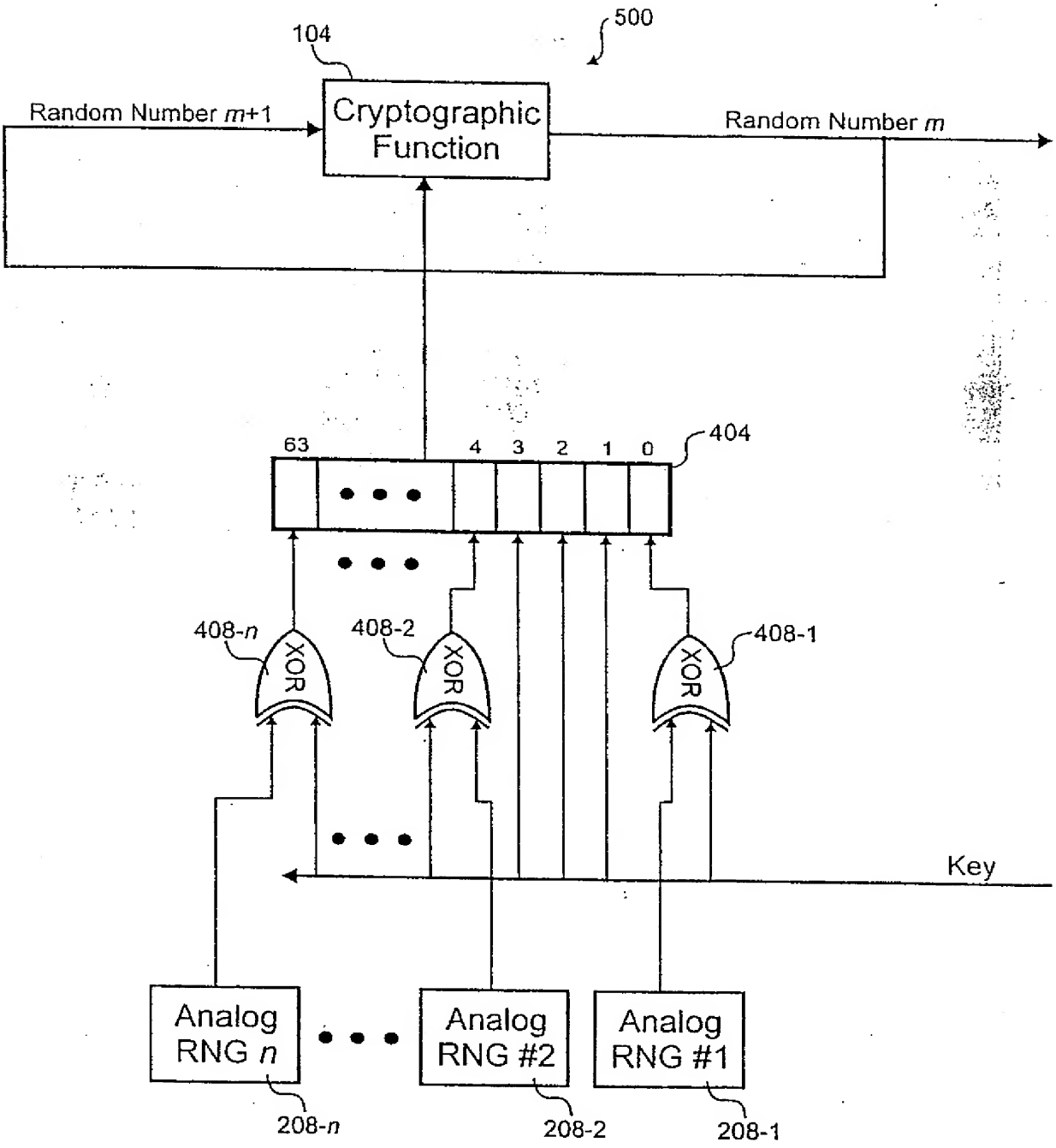


Fig. 5

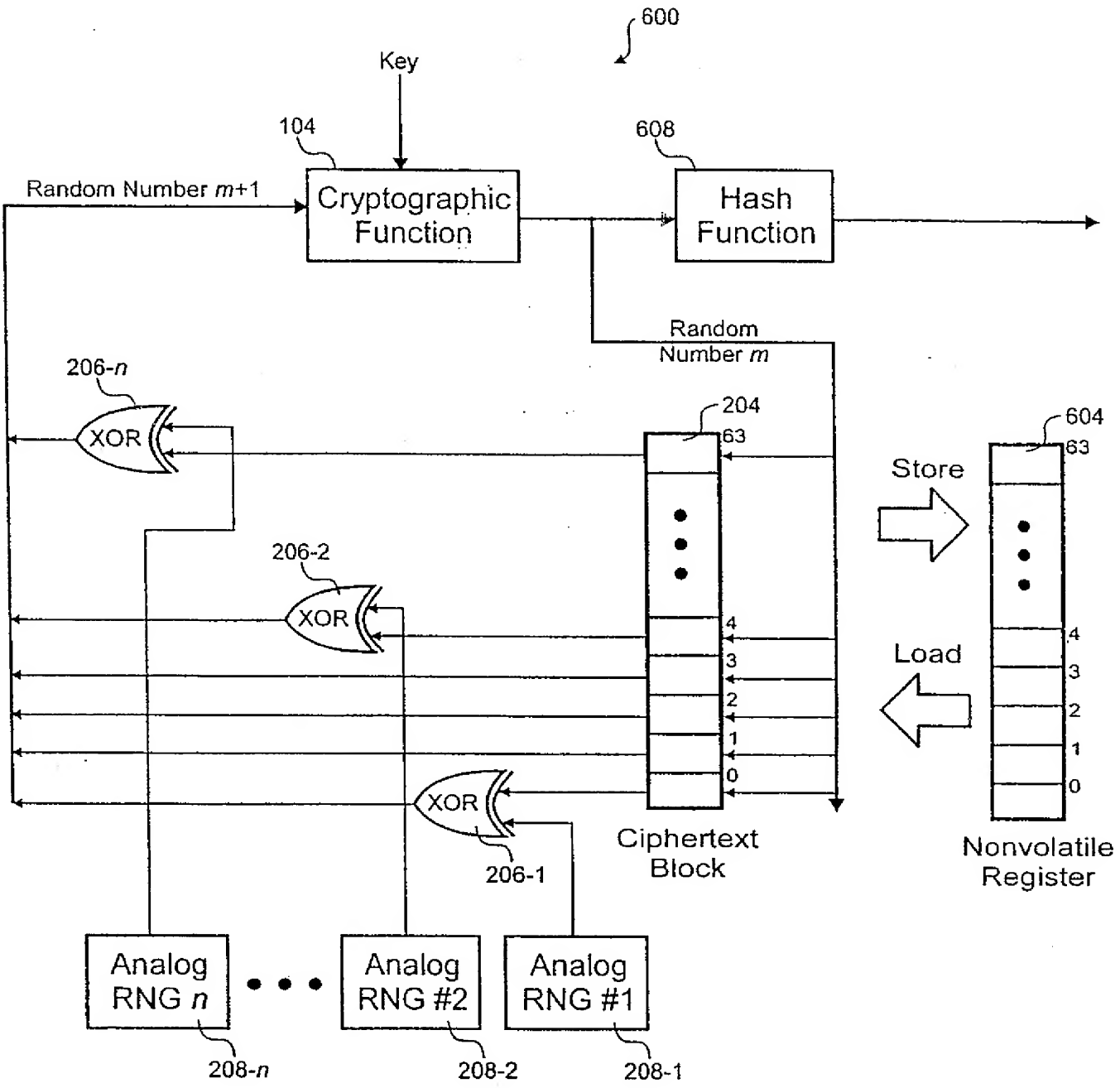


Fig. 6

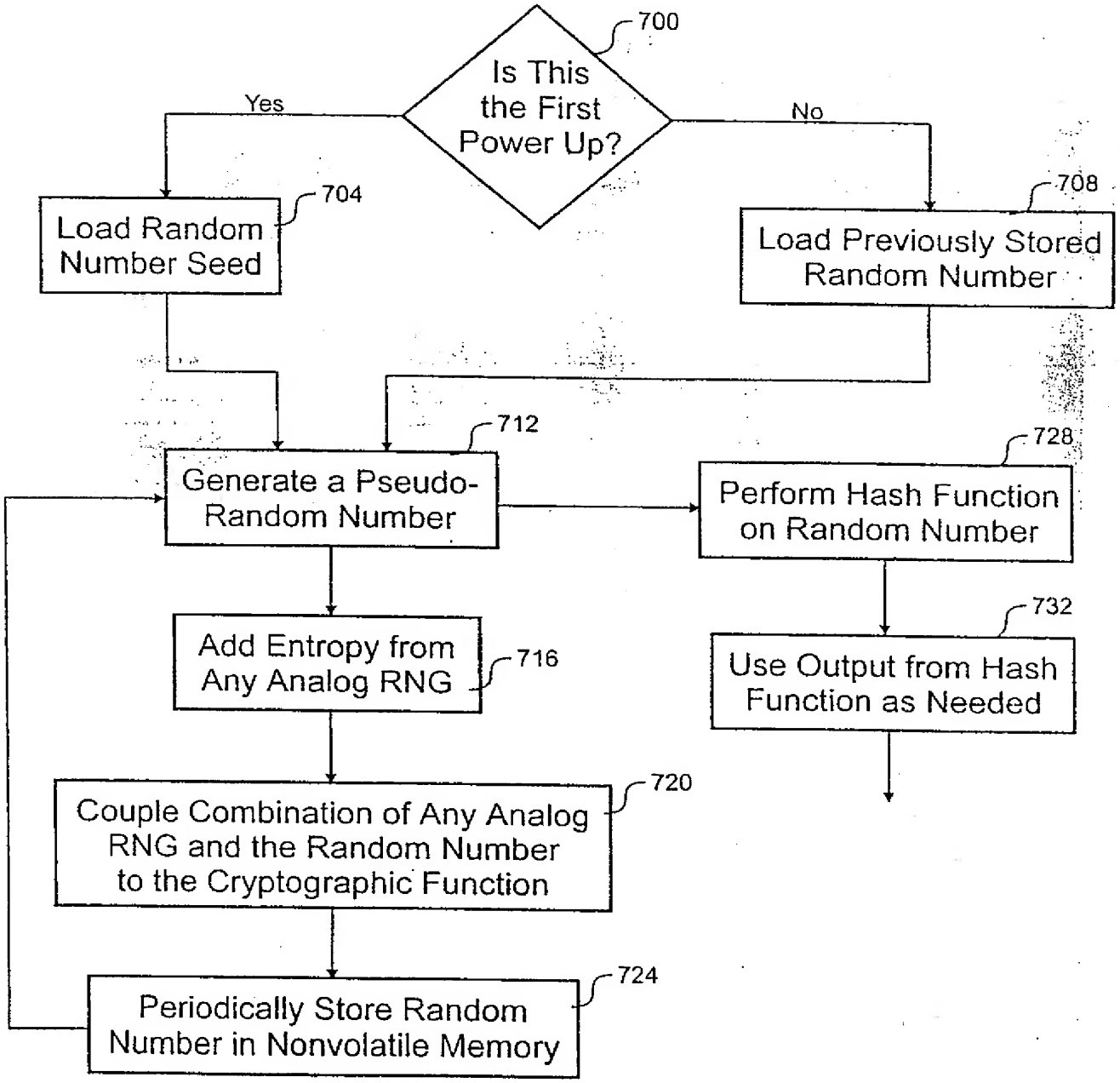


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/15932

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :GO6F 1/02; GO6J 1/00
US CL :708/3, 250

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 708/3, 250-256, 801

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,627,775 A (HONG et al) 06 May 19[illegible] abstract & Fig. 1	1,2, 4-8 & 10-22
X,E	US 6,104,810 A (DEBELLIS etal) 15 August 2000	3 & 9
A,P	US 6,070,178 A (ANDERSON et al) 30 May 2000	1-22

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 24 OCTOBER 2000	Date of mailing of the international search report 16 NOV 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer D. H. MALZAHN James R. Matthews Telephone No. (703) 305-9762

Form PCT/ISA/210 (second sheet) (July 1998)★